CASE STUDY

Leading Australian University Expands Device Awareness and Increases Asset Security

Specialized devices in multiple departments present a visibility challenge for cybersecurity teams

Industry

Higher education

IT environment

300,000 assets, including IT, OT, and MT

Introduction

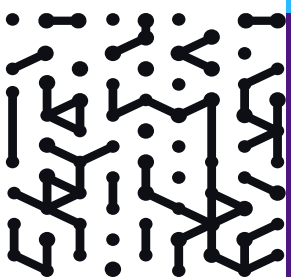
This leading public university in Australia that specializes in technology needed visibility into its vast network of assets to strengthen its security posture and reduce the risk of cyber incidents. Unlike K-12 or other education tiers, this university serves a wide range of disciplines that require a multitude of devices for the courses of study it offers. Armis gave the university unprecedented visibility into network assets that far surpassed expectations, secured the network, and enhanced faculty communication.

This public university based in Australia offers undergraduate, graduate, and postgraduate programs primarily in technical fields—from information technology and engineering to health and science and mathematics. It

has a student body of 45,000 students across nine schools and campuses around the world. As a result of collaborations with private industry in and beyond Australia, the university is operating much like an enterprise.

A small team is responsible for cybersecurity, including operations, management of technical tools, and governance. With its wide range of educational disciplines, asset sprawl comes with the territory. The devices used by students, faculty, and employees are as diverse as the subject areas, spanning traditional IT and operational technology (OT), such as building management systems, microphones, and heavy water fridges, to the more specialized technology, which encompasses engineering and robotics devices and medical technology (MT), such as microscopes and spectrometers. The list of network-connected devices continues to grow.

In this dynamic environment, reaching the ideal device security posture of “known and trusted” has been an ongoing challenge for the security team. After holding various security roles at the university for over 15 years, the cyber operations manager is well aware of the complexities involved in identifying and remediating security threats. He knew that a multitude of devices existed but had no visibility into them. Stretched for time and resources, the cyber operations manager and his team initiated a proof-of-value (PoV) focused on increasing visibility, identifying unknown devices, and defining a remediation path.



Lack of visibility and architecture requirements lead to Armis PoV

The cybersecurity team initially considered an open-source tool but, considering the volume of devices and the number of connections, it soon became apparent that this option wouldn't be suitable. They also evaluated other commercially available tools and found they had limitations. Because the university's network environment does not support switched port analyzer (SPAN) ports, this narrowed the available choices.

Knowing the university's specific implementation needs, a partner introduced the team to Armis, and, thanks to a simple setup, they were able to begin PoV quickly. Prior to the PoV, the cybersecurity team undertook a network detection and response (NDR) initiative, which established the architecture necessary to implement Armis.

"It was fortuitous for Armis that we had done work on network architecture ahead of time and had begun to mirror interconnects between buildings and floors. It made it quite easy to create a feed straight from there into the two Armis devices in our data center without having to put in listeners," the cyber operations manager said.

Armis identifies unknown devices, making risk manageable

Going into the PoV, the team expected a high number of devices on the network. First guesses were around 80,000 devices. Within the first two weeks they had unprecedented visibility and, at the highest count, identified 300,000 devices. "This was the biggest revelation—the time to value was immediate. Once we were plugged in, Armis solved a significant piece of our visibility challenge," the cyber operations manager observed.

The team continued to test and validate the data collected by Armis over six months, building an awareness of devices they had no

Challenges

- Gaining visibility into a wide range of assets
- Increasing faculty awareness of cyber risk
- Identifying vulnerabilities
- Defining a path toward faster remediation

idea about. “The unknown unknowns became known knowns,” the cyber operations manager said. “And the more we know, the more we want to know, and the more we want to do.”

The primary use case the team was solving centered on identifying various workloads in the environment and then differentiating between them. To understand where traffic was going and what the associated risks were, the team began separating devices into buckets: standard operating environment (SOE) devices, managed devices, lab machines, server environments, and more.

As a senior manager at the university, the cyber operations manager knew the value of communicating risk in a language that could be measured and quantified.

“Executives are more receptive to remediation once the threat is quantified. We can then understand the best way to manage the risk, which may look like a segregation strategy into zones of ‘trust’ or ‘untrust.’ This gives us a strong metric to take into conversations with other departments and discuss how to operationalize the data,” the cyber operations manager noted.

Putting threat data to work

One such instance occurred when Armis identified active ransomware on the network. Using an agentless approach and advanced passive listening technologies, Armis detected a threat that would have otherwise been invisible. Because the threat was identified, the team was able to track it down. Armis located unmanaged devices at various departments with obsolete operating systems running on microscopes or similar types of devices. As the cyber operations manager pointed out, since every possible variation of network device can be found at the university, this scenario is not uncommon.

“We’ve gained an unprecedented level of awareness that wasn’t possible before Armis. Now we can pull reports and identify systems for remediation to take into conversations with executives. Armis is an invaluable tool to explain sprawl and the potential threat footprint and risk profile of specific areas of the university. When we meet with faculty, we can easily show the risk on a dashboard—it’s nice and simple,” the cyber operations manager said.

The team had an opportunity to put that into practice recently when they sent executives a report of all devices detected in a faculty members’ building. The general manager called back immediately, stunned by the unexpectedly high number. The faculty kicked off work internally to remediate issues and then followed up asking for another report. Going forward, the team is considering providing the faculty with access so they can pull this data on their own.

“We’ve gained an unprecedented level of awareness that wasn’t possible before Armis. Now we can pull reports and identify systems for remediation to take into conversations with executives. Armis is an invaluable tool to explain sprawl and the potential threat footprint and risk profile of specific areas of the university. When we meet with faculty, we can easily show the risk on a dashboard—it’s nice and simple.”

Cyber Operational Manager
University of Technology

Moving forward with integrations and broad support

One of the key integrations the university has completed is with a managed security operations center (SOC), which provides 24/7 real-time monitoring and data analysis along with incident management and remediation. Through this integration with Armis, the university can further improve its security posture.

Armis is also integrated with the Palo Alto Networks Prisma Cloud tool, which provides comprehensive visibility, threat detection/prevention, compliance assurance, and data protection for hybrid and multi-cloud environments. Armis data is correlated with data sources from major cloud platforms.

Remediation by leveraging the capability to quarantine devices from the network through Armis will be explored, as the team look to expand its capability. As the platform matures, the goal is to communicate with teams outside of security to support remediation. "Within the university, we have broad visibility and an ingrained understanding that 'A' plus 'B' may equal 'X,' but communicating that can be a challenge, especially when classroom tools are impacted," the cyber manager said.

The more the team can frame risk and share metrics, the easier their task will become. These integrations are undoubtedly helping the university work toward a single source of truth. Once they are completed, the team plans to tackle the task of how best to operationalize this data in order to gain an understanding of what they can do with it and where they can make improvements. As a small team, they'll continue to rely on strong partnerships to solve problems.

"Being a small team challenged by lack of time, we appreciate the assistance provided by the Armis team. We always have too much to do and too little time. Armis is proactive and always sought to improve the deployment with workshops and integrations. They've helped cement the product into our environment, in part because Armis is invested in our success," the cyber operations manager noted.

Armis Results

- Discovered a large volume of previously unknown network-connected devices
- Gained an awareness of the threat footprint
- Improved cross-department collaboration
- Drove more effective remediation through threat data analysis and correlation
- Gained an integrated investigative tool

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial